Domande frequenti e guida alla risoluzione dei problemi di CX Cloud Agent

Sommario

Introduzione

Questo documento include le domande frequenti e gli scenari di risoluzione dei problemi che gli utenti possono incontrare quando utilizzano l'agente cloud CX.

Implementazione

D. Il reindirizzamento dell'URL a cloudfront.net è un comportamento previsto quando ci si connette al dominio back-end di CX Cloud?

R. Sì, per alcuni scenari di distribuzione specifici il reindirizzamento a cloudfront.net è previsto. Ol'accesso non associato deve essere consentito con il reindirizzamento abilitato sulla porta 443 per questi FQDN.

D. Con l'opzione "Re-install", l'utente può implementare il nuovo agente cloud CX con un nuovo indirizzo IP?

A. Sì

D. Quali formati di file sono disponibili per l'installazione?

A. OVA e VHD

D. In quale ambiente è possibile installare l'installabile?

R. Per gli OVULI

- VMware ESXi versione 5.5 o successiva
- Oracle Virtual Box 5.2.30 o successivo

Per VHD

- Windows Hypervisor da 2012 a 2016

D. L'agente cloud CX può rilevare un indirizzo IP in un ambiente DHCP?

R. Sì, viene rilevata l'assegnazione dell'indirizzo IP durante la configurazione IP. Tuttavia, la modifica dell'indirizzo IP prevista per l'agente cloud CX in futuro non è supportata. Si consiglia di riservare l'IP per l'agente cloud CX nell'ambiente DHCP.

D. L'agente cloud CX supporta la configurazione IPv4 e IPv6?

R. No, è supportato solo il protocollo IPV4.

D. Durante la configurazione IP, l'indirizzo IP viene convalidato?

R. Sì, vengono convalidati la sintassi degli indirizzi IP e l'assegnazione di indirizzi IP duplicati.

D. Quanto tempo è necessario per l'installazione degli OAV e la configurazione IP?

A.La distribuzione degli OAV dipende dalla velocità della rete che copia i dati. La configurazione IP richiede all'incirca 8-10 minuti, inclusi Kubernetes e la creazione di container.

D. Sono previste limitazioni per i tipi di hardware?

R. Il computer host su cui è distribuito OVA deve soddisfare i requisiti forniti nell'ambito della configurazione del portale CX. L'agente cloud CX viene testato con VMware/Virtual box in esecuzione su un hardware con processori Intel Xeon E5 con rapporto vCPU/CPU impostato su 2:1. Se si utilizza una CPU del processore meno potente o un rapporto maggiore, le prestazioni possono peggiorare.

D. È possibile generare il codice di associazione in qualsiasi momento?

R. No, il codice di associazione può essere generato solo quando l'agente cloud CX non è registrato.

D. Quali sono i requisiti di larghezza di banda tra Cisco DNA Center (per un massimo di 10 cluster o 20 non cluster) e CX Cloud Agent?

A.La larghezza di banda non è un vincolo quando l'agente cloud CX e Cisco DNA Center si trovano nella stessa rete LAN/WAN nell'ambiente del cliente. La larghezza di banda di rete minima richiesta è 2,7 Mbit/sec per le raccolte di inventario di 5000 dispositivi + 13000 access point per la connessione di un agente a Cisco DNA Center. Se i syslog vengono raccolti per le informazioni di livello 2, la larghezza di banda minima richiesta è 3,5 Mbit/sec per le coperture di 5000 dispositivi +13000 Access Point per inventario, 5000 dispositivi syslog e 2000 dispositivi per scansioni, il tutto eseguito in parallelo da CX Cloud Agent.

D. Modalità di syslog dell'agente è possibile accedere per il monitoraggio della macchina virtuale (VM) dell'agente cloud CX?

R. È possibile accedere ai syslog per la macchina virtuale dell'agente dall'accesso alla macchina virtuale locale utilizzando i due percorsi seguenti:

/var/log/syslog.1 (accesso tramite cxcadmin e cxcroot login)

/var/log/syslog (accesso tramite root)

Release e patch

D. Quali sono i diversi tipi di versioni elencate per l'aggiornamento di CX Cloud Agent?

R. Di seguito sono elencate le versioni rilasciate di CX Cloud Agent:

- A.x.0 (dove x è l'ultima versione della principale funzionalità di produzione, ad esempio, 1.3.0)
- A.x.y (dove A.x.0 è obbligatorio e deve essere avviato l'aggiornamento incrementale, x è l'ultima versione delle funzionalità principali di produzione e y è l'ultima patch di aggiornamento disponibile, ad esempio 1.3.1)
- A.x.y-z (dove A.x.0 è obbligatorio e deve essere avviato l'aggiornamento incrementale, x è l'ultima versione delle funzionalità principali di produzione, e y è l'ultima patch di

aggiornamento disponibile e z è la patch spot che è una correzione istantanea per un periodo di tempo molto breve, ad esempio: 1.3.1-1)

dove A è una release a lungo termine distribuita su 3-5 anni.

D. Dove trovare la versione più recente rilasciata di CX Cloud Agent e come aggiornare l'agente CX Cloud esistente?

R. Accedere al portale CX Cloud. Passare a Impostazioni amministratore>Origini dati. Fare clic su View Update (Visualizza aggiornamento) e seguire le istruzioni visualizzate.

Autenticazione e configurazione del proxy

D. Qual è l'utente predefinito per l'applicazione CX Cloud Agent?

A. cxcadmin

D. Come viene impostata la password per l'utente predefinito?

R. Le password vengono impostate durante la configurazione della rete.

D. È disponibile un'opzione per reimpostare la password dopo il giorno 0?

R. L'agente cloud CX non fornisce alcuna opzione specifica per reimpostare la password, ma è possibile utilizzare i comandi Linux per reimpostare la password per cxcadmin.

D. Quali sono i criteri password per configurare l'agente CX Cloud?

R. I criteri per la password sono:

- Durata massima (lunghezza) impostata su 90 giorni
- Età minima (lunghezza) impostata su 8 giorni
- Lunghezza massima 127 caratteri
- È necessario includere almeno un carattere maiuscolo e uno minuscolo
- Deve contenere almeno un carattere speciale, ad esempio !$%^&*()_+|~-=\`{}[]:";'<>?,/)
- I caratteri seguenti non sono consentiti
    - Caratteri speciali a 8 bit (ad esempio, ¬£, √ √ ', √¥, √ ë, SUDDIVISIONE, √ ü)
    - Spazi
- Non devono essere le ultime 10 password utilizzate di recente
- Non deve contenere espressioni regolari
- Non deve contenere le seguenti parole o derivati: cisco, sanjose, and sanfran

D. Come posso verificare la raggiungibilità di Secure Shell (SSH) su un dispositivo da CX Cloud Agent?

A. Per confermare la raggiungibilità SSH:

1. Accedi come utente di Cxcroot.
2. Eseguire il comando seguente per abilitare la porta SSH in Iptables:

Iptables -A OUTPUT -p tcp -m tcp —dport 22 -j ACCEPT

3. Per verificare la raggiungibilità SSH, eseguire il comando seguente:

ssh user@ip-address:porta

Per disabilitare le porte SSH abilitate in precedenza nell'agente cloud CX:

1. Eseguire il comando seguente per ottenere il numero di riga della porta SSH abilitata nelle tabelle IP:

iptables -L OUTPUT —numero-riga | dpt grep | grep ssh | sveglio '{print $1}'

2. Eseguire il comando seguente per eliminare il numero di riga ottenuto:

iptables -L OUTPUT <numero riga>

D. Come posso confermare la raggiungibilità SNMP su un dispositivo da CX Cloud Agent?

R. Per confermare la raggiungibilità di SNMP:

1. Accedi come utente di Cxcroot.
2. Eseguire il comando seguente per abilitare le porte SNMP nelle tabelle IP:

iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

iptables -A OUTPUT -p udp -m udp —dport 161 -j ACCEPT

3. Eseguire il comando snmpwalk/snmpget seguente per confermare la raggiungibilità del protocollo SNMP:

snmpwalk -v2c -c indirizzo IP cisco

Per disabilitare le porte SNMP abilitate in precedenza nell'agente cloud CX:

1. Eseguire il comando seguente per ottenere i numeri di riga delle porte SNMP abilitate (come risposta vengono generati due numeri di riga):

iptables -L OUTPUT —numero-riga | dpt grep | grep ssh | sveglio '{print $1}'

2. Eseguire il comando seguente per eliminare i numeri di riga (in ordine decrescente):

iptables -L OUTPUT <numero riga2 Numero>

iptables -L OUTPUT <numero riga1 Numero>

D. Come è possibile impostare la password di Grub?

A. Per impostare la password di Grub:

1. Eseguire ssh come cxcroot e fornire il token [contattare il team di supporto per ottenere il token cxcroot].
2. Eseguire sudo su, per fornire lo stesso token.
3. Eseguire il comando grub-mkpasswd-pbkdf2 e impostare la password di Grub. Verrà stampato un hash della password fornita, copiare il contenuto.
4. vi nel file /etc/grub.d/00_header.
5. Passare alla fine del file e sostituire l'output dell'hash seguito dal contenuto password_pbkdf2 root ***** con l'hash ottenuto per la password ottenuto nel passaggio 3.
6. Salvate il file con il comando :wq!.
7. Eseguire il comando update-grub.

D. Qual è il periodo di scadenza per la password cxcadmin?

R. La password scade tra 90 giorni.

D. Il sistema disabilita l'account dopo tentativi consecutivi di login non riusciti?

R. Sì, l'account viene disabilitato dopo cinque (5) tentativi consecutivi non riusciti. L'account viene bloccato per 30 minuti.

D. Come è possibile generare una passphrase?

A. Per generare una passphrase:

1. Esegui .ssh e accedi come utente cxcadmin
2. Eseguire il comando remoteaccount cleanup -f
3. Eseguire il comando create dell'account remoto

D. L'host proxy supporta sia il nome host che l'indirizzo IP?

R. Sì, ma per utilizzare il nome host, l'utente deve fornire l'indirizzo IP DNS (Domain Name Server) durante la configurazione della rete.

Secure Shell (SSH)

D. Quali cifrari sono supportati dalla shell ssh?

R. Sono supportati i seguenti cifrari:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

D. Come si accede alla console?

A. Per accedere:

1. Accedi come utente cxcadmin
2. Specificare la password cxcadmin

D. Gli accessi SSH sono registrati?

R. Sì, sono registrati come parte del file "var/logs/audit/audit.log".

D. Qual è il timeout della sessione di inattività?

R. Il timeout della sessione SSH si verifica se l'agente cloud CX rimane inattivo per cinque (5) minuti.

Porte e servizi

D. Quali porte rimangono aperte sull'agente cloud CX?

R. Sono disponibili le seguenti porte:

- Porta in uscita: l'agente cloud CX implementato può connettersi al back-end Cisco come indicato nella tabella sulla porta HTTPS 443 o tramite un proxy per inviare i dati a Cisco come indicato nella tabella seguente. L'agente cloud CX implementato può connettersi a Cisco DNA Center sulla porta HTTPS 443.

AMERICAS	EMEA	APJC
cloudsso.cisco.com	cloudsso.cisco.com	cloudsso.cisco.com
api-cx.cisco.com	api-cx.cisco.com	api-cx.cisco.com
agent.us.csco.cloud	agente.emea.cisco.cloud	agente.apjc.cisco.cloud
ng.acs.agent.us.csco.cloud	ng.acs.agent.emea.cisco.cloud	ng.acs.agent.apjc.cisco.cloud

Nota: oltre ai domini elencati, quando i clienti EMEA o APJC reinstallano l'agente cloud CX, il dominio agent.us.csco.cloud deve essere consentito nel firewall del cliente.
Il dominio agent.us.csco.cloud non è più necessario dopo la corretta reinstallazione.

Nota: verificare che il traffico di ritorno sia consentito sulla porta 443.

- Inbound port: per la gestione locale dell'agente cloud CX, devono essere accessibili 514 (Syslog) e 22 (ssh). I clienti devono consentire alla porta 443 nel proprio firewall di ricevere i dati da CX Cloud.

Rapporto tra CX Cloud Agent e Cisco DNA Center

D. Qual è lo scopo e la relazione di Cisco DNA Center con CX Cloud Agent?

R. Cisco DNA Center è l'agente cloud che gestisce i dispositivi di rete della sede del cliente. CX Cloud Agent raccoglie le informazioni di inventario dei dispositivi dal Cisco DNA Center configurato e carica le informazioni di inventario disponibili nella Asset View di CX Cloud.

D. Dove possono gli utenti fornire i dettagli Cisco DNA Center sull'agente cloud CX?

R. Durante il Giorno 0 - Installazione di CX Cloud Agent, gli utenti possono aggiungere i dettagli di Cisco DNA Center dal portale CX Cloud. Durante le operazioni del Giorno N, gli utenti possono aggiungere altri Cisco DNA Center da Admin Settings > Data Source.

D. Quanti Cisco DNA Center è possibile aggiungere?

R. È possibile aggiungere dieci (10) cluster Cisco DNA Center o 20 non cluster Cisco DNA Center.

D. Come rimuovere un Cisco DNA Center connesso da CX Cloud Agent?

R. Per rimuovere un Cisco DNA Center connesso dall'agente cloud CX, contattare il Technical Assistance Center (TAC) per aprire una richiesta di assistenza dal portale cloud CX.

D. Quale ruolo può svolgere l'utente Cisco DNA Center?

R. Il ruolo utente può essere admin o observer.

D. In che modo le modifiche apportate all'agente cloud CX a causa delle modifiche delle credenziali di un DNA Center connesso?

R. Eseguire il comando cxcli agent modifyController dalla console dell'agente cloud CX:

Contattare il supporto tecnico per qualsiasi problema durante l'aggiornamento delle credenziali di Cisco DNA Center.

D. Come vengono archiviati i dettagli degli asset di Cisco DNA Center e dei file di inizializzazione in CX Cloud Agent?

R. Tutti i dati, incluse le credenziali dei controller connessi all'agente cloud CX (ad esempio, Cisco DNA Center) e gli asset connessi direttamente (ad esempio, tramite file di inizializzazione,

intervallo IP), vengono crittografati utilizzando AES-256 e archiviati nel database dell'agente cloud CX che è protetto con un ID utente e una password protetti.

D. Che tipo di crittografia viene utilizzata durante l'accesso all'API Cisco DNA Center da CX Cloud Agent?

R. HTTPS over TLS 1.2 viene utilizzato per la comunicazione tra Cisco DNA Center e l'agente CX Cloud.

D. Quali operazioni vengono eseguite dall'agente cloud CX sull'agente cloud Cisco DNA Center integrato?

R. L'agente cloud CX raccoglie dati dai Cisco DNA Center sui dispositivi di rete e utilizza l'interfaccia di esecuzione dei comandi di Cisco DNA Center per comunicare con i dispositivi terminali ed eseguire i comandi CLI (comando show). Non viene eseguito alcun comando di modifica della configurazione.

D. Quali dati predefiniti vengono raccolti da Cisco DNA Center e caricati nel back-end?

R.

- Entità di rete
- Moduli
- Show version
- Config
- Informazioni sull'immagine del dispositivo
- Tag

D. Quali dati aggiuntivi vengono raccolti da Cisco DNA Center e caricati nel back-end Cisco?

R. Per ulteriori informazioni, consultare il documento.

D. Come vengono caricati i dati di inventario nel back-end?

R. CX Cloud Agent carica i dati di inventario tramite il protocollo TLS 1.2 sul server back-end Cisco.

D. Qual è la frequenza di caricamento delle scorte?

R. La raccolta viene attivata in base alla pianificazione definita dall'utente e caricata nel back-end Cisco.

D. L'utente può riprogrammare l'inventario?

R. Sì, è disponibile un'opzione da Impostazioni amministratore > Origini dati per modificare le informazioni di pianificazione.

D. Quando si verifica il timeout della connessione tra Cisco DNA Center e Cloud Agent?

A. I timeout sono classificati come segue:

- Per la connessione iniziale, il timeout è un massimo di 300 secondi. Se non viene stabilita una connessione tra Cisco DNA Center e Cloud Agent entro un massimo di cinque (5) minuti, la connessione viene terminata.
- Per aggiornamenti ricorrenti, tipici o: il timeout di risposta è 1800 secondi. Se la risposta non viene ricevuta o non può essere letta entro 30 minuti, la connessione viene terminata.

Analisi diagnostica di CX Cloud Agent

D. Quali comandi di scansione vengono eseguiti sul dispositivo?

R. I comandi che devono essere eseguiti sul dispositivo per la scansione vengono determinati in modo dinamico durante il processo di scansione. L'insieme di comandi può cambiare nel tempo, anche per lo stesso dispositivo (e non in controllo di Diagnostic Scan).

D. Dove vengono archiviati e analizzati i risultati dell'analisi?

R. I risultati della scansione vengono archiviati e analizzati nel back-end Cisco.

D. I duplicati (per nome host o IP) in Cisco DNA Center vengono aggiunti alla scansione diagnostica quando è collegata l'origine Cisco DNA Center?

R. No, i duplicati vengono filtrati in modo da estrarre solo i dispositivi univoci.

D. Cosa succede quando una delle analisi dei comandi ha esito negativo?

R. La scansione del dispositivo si interrompe completamente e viene contrassegnata come non riuscita.

Log di sistema di CX Cloud Agent

D. Quali informazioni sullo stato vengono inviate al portale CX Cloud?

R. Registri delle applicazioni, stato dei dispositivi, dettagli di Cisco DNA Center, registri di verifica, dettagli di sistema e dettagli hardware.

D. Quali dettagli relativi al sistema e all'hardware vengono raccolti?

A. Output di esempio:

system_details":{
"os_details":{
"containerRuntimeVersion":"docker://19.3.12",
"kernelVersion":"5.4.0-47-generic",
"kubeProxyVersion":"v1.15.12",
"kubeletVersion":"v1.15.12",
"machineID":"81edd7df1c1145e7bcc1ab4fe78615f",
"operatingSystem":"linux",
"osImage":"Ubuntu 20.04.1 LTS",
"systemUUID":"42002151-4131-2ad8-4443-8682911bdadb"
},
"dettagli_hardware":{
"total_cpu":"8",
"cpu_usage":"12,5%",
"total_memory":"1607 MB",
"free_memory":"9994 MB",
"hdd_size":"214G",
"free_hdd_size":"202G"
}
}
}

D. Come vengono inviati i dati di integrità al back-end?

R. Con l'agente cloud CX, il servizio di integrità (facilità di manutenzione) invia i dati al back-end Cisco.

D. Quali sono le regole di conservazione dei log di dati sullo stato dell'agente cloud CX nel back-end?

R. Il criterio di conservazione del log di dati sull'integrità dell'agente cloud CX nel back-end è di 120 giorni.

D. Quali tipi di caricamento sono disponibili?

R.

1. Caricamento scorte
2. Caricamento syslog
3. Caricamento dell'integrità dell'agente, incluso il caricamento dell'integrità
    1. Integrità dei servizi: ogni cinque (5) minuti
    2. Podlog - Ogni (1) ora
    3. Registro di controllo - Ogni (1) ora

Risoluzione dei problemi

Problema: impossibile accedere all'indirizzo IP configurato.

Soluzione: eseguire ssh utilizzando l'IP configurato. In caso di timeout della connessione, è possibile che l'indirizzo IP non sia stato configurato correttamente. In questo caso, eseguire nuovamente l'installazione configurando un indirizzo IP valido. A tale scopo, è possibile utilizzare il portale con l'opzione di reinstallazione fornita nel Admin Settingspagina.

Problema: come posso verificare che i servizi siano attivi e in esecuzione dopo la registrazione?

Soluzione: per verificare che i pod siano attivi e in esecuzione, procedere come segue:

1. Eseguire il comando SSH sull'IP configurato come cxcadmin
2. Immettere la password
3. Eseguire il comando kubectl get pods

I pod possono essere in qualsiasi stato (in esecuzione, inizializzazione o creazione di contenitori). Dopo 20 minuti, i baccelli devono essere in stato In esecuzione.

Se lo stato non è in esecuzione o Pod Initializing, controllare la descrizione del pod con il comando kubectl description pod <podname>.

L'output conterrà informazioni sullo stato del pod.

Problema: come verificare se l'intercettore SSL è disabilitato sul proxy del cliente?
Soluzione: eseguire il comando curl illustrato per verificare la sezione relativa al certificato del server. La risposta contiene i dettagli del certificato del server Web concavo.

curl -v —header 'Authorization: Basic xxxxxx' https://concsoweb-prd.cisco.com/

* Certificato server:

* soggetto: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=concsoweb-prd.cisco.com

* data di inizio: 16 febbraio 11:55:11 2021 GMT

* data di scadenza: 16 febbraio 12:05:00 2022 GMT

* subjectAltName: l'host "concsoweb-prd.cisco.com" corrisponde al certificato "concsoweb-prd.cisco.com"

* autorità emittente: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL CA G3

* Il certificato SSL è valido.

> GET/HTTP/1.1

Problema: i comandi kubectl non sono riusciti e mostrano l'errore come "La connessione al server X.X.X.X:6443 è stata rifiutata - sono stati specificati l'host o la porta corretti"
Soluzione:

- Verificare la disponibilità delle risorse, [esempio: CPU, Memoria].
- Attendere l'avvio del servizio Kubernetes.

Problema: come ottenere i dettagli dell'errore di raccolta per un comando o un dispositivo?

Soluzione:

- Immettere il comando `kubectl get pods` e richiamare il nome del pod di raccolta.
- Immettere il comando `kubectl logs` per ottenere i dettagli specifici del comando o del dispositivo.

Problema: il comando kubectl non funziona con l'errore "[authentication.go:64] Impossibile autenticare la richiesta a causa di un errore: [x509: certificato scaduto o non ancora valido, x509: certificato scaduto o non ancora valido]"

Soluzione:eseguire i comandi visualizzati come utente cxcroot

rm /var/lib/rancher/k3s/server/tls/dynamic-cert.json
systemctl restart k3s
kubectl —insecure-skip-tls-verify=true delete secret -n kube-system k3s-serving
systemctl restart k3s

Risoluzione degli errori di raccolta

L'errore di raccolta può essere causato da qualsiasi vincolo o problema riscontrato nel controller aggiunto o nei dispositivi presenti nel controller.

Nella tabella riportata di seguito è riportato il frammento di codice di errore relativo ai casi di utilizzo rilevati nel microservizio Collection durante il processo di raccolta.

Scenario d'uso	Frammento di codice nel log del microservizio Collection

Il dispositivo desiderato non viene rilevato in Cisco DNA Center	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": " Nessun dispositivo trovato con ID 02eb08be-b13f-4d25-9d63-eaf4e882f71a "
	}

Il dispositivo desiderato non è raggiungibile da Cisco DNA	{ "command": "show version",

Scenario d'uso	Frammento di codice nel log del microservizio Collection
Center	"status": "Failed" (Non riuscito), "commandResponse": "", "errorMessage": "Errore durante l'esecuzione del comando: show version\nErrore durante la connessione al dispositivo [Host: 172.21.137.221:22]Nessuna route all'host: nessuna route all'host " }

Il dispositivo desiderato non è raggiungibile da Cisco DNA Center	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Errore durante l'esecuzione del comando: show version\nErrore durante la connessione al dispositivo [Host: X.X.X.X]Timeout connessione: /X.X.X.X:22 : Timeout connessione: /X.X.X.X:22"
	}

Se il comando richiesto non è disponibile nel dispositivo	{
	"command": "show run-config",
	"status": "Operazione riuscita",
	"commandResponse": " Errore durante l'esecuzione del comando: show run-config\n\nshow run-config\n ^\n% Input non valido rilevato in \u0027^\u0027 marker.\n\nXXCT5760#",
	"messaggio di errore": ""
	}

Se il dispositivo richiesto non dispone di SSHv2 e Cisco DNA Center tenta di connetterlo con SSHv2	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Errore durante l'esecuzione del comando: show version\nCanale SSH2 chiuso: la parte remota utilizza un protocollo incompatibile, non è compatibile SSH-2."
	}

Il comando è disabilitato nel microservizio Collection	{ "command": "config paging disable", "status": "Command_Disabled", "commandResponse": "Raccolta comandi disabilitata", "messaggio di errore": ""

Scenario d'uso	Frammento di codice nel log del microservizio Collection
	}

Esecuzione dell'attività Command Runner non riuscita, Cisco DNA Center non restituisce l'URL dell'attività	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s. URL attività vuoto."
	}

Creazione dell'attività Command Runner non riuscita in Cisco DNA Center	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s, RequestURL: %s. Nessun dettaglio sull'attività."
	}

Se il microservizio Collection non riceve una risposta per una richiesta di Command Runner da Cisco DNA Center	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s, RequestURL: %s."
	}

Cisco DNA Center non completa l'attività entro il timeout configurato (5 minuti per comando nel microservizio Collection)	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Timeout operazione. Attività del router dei comandi non riuscita per il dispositivo %s, RequestURL: %s. Nessun dettaglio sull'avanzamento."
	}

Se l'operazione Command Runner non è riuscita e l'ID file è vuoto per l'operazione inviata da Cisco DNA Center	{ "command": "show version", "status": "Failed" (Non riuscito), "commandResponse": "",

Scenario d'uso	Frammento di codice nel log del microservizio Collection
	"errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s, RequestURL: %s. ID file vuoto." }

Se l'operazione Command Runner non è riuscita e il tag ID file non viene restituito da Cisco DNA Center	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s, RequestURL: %s. Nessun dettaglio dell'ID file."
	}

Command Runner non può essere eseguito sul dispositivo	{
	"command": "config paging disable",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "I dispositivi richiesti non sono in inventario, prova con altri dispositivi disponibili in inventario"
	}

Command Runner non può essere eseguito dall'utente	{
	"command": "show version",
	"status": "Failed" (Non riuscito),
	"commandResponse": "",
	"errorMessage": "{\"messaggio\":\"Il ruolo non dispone di autorizzazioni valide per accedere all'API\"}\n"
	}

Risoluzione degli errori di analisi diagnostica

Gli errori di scansione e le cause possono essere da uno qualsiasi dei componenti elencati.

Quando gli utenti avviano un'analisi dal portale, a volte viene restituito il messaggio "operazione non riuscita: errore interno del server".

La causa del problema è uno dei componenti elencati

- Punto di controllo
- Gateway dei dati della rete
- Connettore

- Analisi diagnostica
- Microservizio di CX Cloud Agent (devicemanager, collection)
- Cisco DNA Center
- APIX
- Mashery
- Accesso ping
- IRONBANK
- IRONBANK GW
- Big Data Broker (BDB)

Per visualizzare i registri:

1. Accedere alla console di CX Cloud Agent.
2. Immettere il comando `kubectl get pods` .
3. Ottenere il nome del pod della raccolta, il connettore e la facilità di manutenzione.
4. Per verificare la raccolta, il connettore e i registri dei microservizi di facilità di manutenzione.

- Immettere il comando `kubectl logs`

- Immettere il comando `kubectl logs`

- Immettere il comando `kubectl logs`

Nella tabella seguente viene visualizzato il frammento di codice di errore presente nei registri del microservizio Raccolta e del microservizio facilità di manutenzione che si verifica a causa dei problemi/vincoli dei componenti.

Scenario d'uso	Frammento di codice nel log del microservizio Collection

Il dispositivo può essere raggiungibile e supportato, ma i comandi da eseguire su tale dispositivo sono elencati a blocchi nel microservizio Collection	{
	"command": "config paging disable",
	"status": "Command_Disabled",
	"commandResponse": "Raccolta comandi disabilitata",
	}

Se il dispositivo per l'analisi non è disponibile. Si verifica in uno scenario in cui esiste un problema di sincronizzazione tra componenti quali portale, analisi diagnostica, componente CX e Cisco DNA Center	Nessun dispositivo trovato con ID 02eb08be-b13f-4d25-9d63-eaf4e882f71a

Scenario d'uso	Frammento di codice nel log del microservizio Collection
Il dispositivo che si sta tentando di analizzare è occupato, in uno scenario in cui lo stesso dispositivo fa parte di un altro processo e Cisco DNA Center non gestisce richieste parallele per il dispositivo	Tutti i dispositivi richiesti sono già stati interrogati dal runner di comandi in un'altra sessione. Provare con altri dispositivi
Il dispositivo non supporta la funzionalità di analisi	I dispositivi richiesti non sono in inventario. Provare con altri dispositivi disponibili in inventario
Se il dispositivo che si è tentato di analizzare non è raggiungibile	"Errore durante l'esecuzione del comando: show udi\nErrore durante la connessione al dispositivo [Host: x.x.x.x:22] Nessuna route all'host: nessuna route all'host
Cisco DNA Center non è raggiungibile dal Cloud Agent oppure il microservizio Collection del Cloud Agent non riceve risposta in seguito a una richiesta Command Runner di Cisco DNA Center	{ "command": "show version", "status": "Failed" (Non riuscito), "commandResponse": "", "errorMessage": "Attività del runner di comando non riuscita per il dispositivo %s, RequestURL: %s." }

Scenario d'uso	Frammento di codice nel log del microservizio Control Point Agent
Nella richiesta di analisi mancano i dettagli della pianificazione	Impossibile eseguire la richiesta {"message":"23502: il valore null nella colonna \"schedulazione\" viola il vincolo not-null"}
Nella richiesta di analisi mancano i dettagli del dispositivo	Impossibile creare il criterio di analisi. Nessun dispositivo valido nella richiesta
Connettività al CPA assente	Impossibile eseguire la richiesta
Il dispositivo da analizzare non supporta le analisi diagnostiche	Impossibile inviare la richiesta di analisi. Motivo = {\"messaggio\":\"Impossibile trovare il dispositivo con

Scenario d'uso	Frammento di codice nel log del microservizio Control Point Agent
	nome host=x.x.x.x\"}

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).